

IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED CON NETHSERVER EN UN ENTORNO VIRTUALIZADO

Yeisson Fernando Rincon Blandon

Email: yfrinconb@unadvirtual.edu.co

Kenny Rafael Guardiola Diaz

Email: krguardioladi@unadvirtual.edu.co

Martín Elías López Pérez

Email: melopezpe@unadvirtual.edu.co

Deivis Antonio Viloría Solano

Email: davilorias@unadvirtual.edu.co

Juan Jose Romero Jimenez

Email: jjromeroj@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación paso a paso de un servidor GNU/Linux con la distribución NethServer 7.9.2009 en una máquina virtual. El objetivo es construir una infraestructura de red robusta y segura que ofrezca servicios de red esenciales como DHCP, DNS, un controlador de dominio y una VPN. Se describe la configuración de un proxy web para filtrar el tráfico de internet y un firewall para bloquear el acceso a sitios no deseados, mejorando la seguridad de la red. Adicionalmente, se detallan los pasos para configurar un servidor de archivos (File Server) y un servidor de impresión (Print Server) para la gestión eficiente de recursos compartidos. La VPN permite el acceso remoto seguro a la red, proporcionando una capa adicional de seguridad y privacidad. Se incluyen pruebas de validación para comprobar el correcto funcionamiento de cada servicio, asegurando que la infraestructura cumple con los requisitos de seguridad y funcionalidad [7].*

PALABRAS CLAVE: GNU/Linux, NethServer, Virtualización, Seguridad de red, Red local, Servidor DHCP, Servidor DNS, Controlador de Dominio, Proxy Web, Firewall, File Server, Print Server, VPN.

ABSTRACT: *This article presents a step-by-step implementation of a GNU/Linux server using the NethServer 7.9.2009 distribution in a virtual machine. The goal is to build a robust and secure network infrastructure that offers essential network services such as DHCP, DNS, a domain controller, and a VPN. The configuration of a web proxy to filter internet traffic and a firewall to block access to unwanted sites is described, thus improving network security. Additionally, the steps to configure a file server and a print server for efficient management of shared resources are detailed. The VPN allows secure remote access to the network, providing an additional layer of security and privacy. Validation tests are included to verify the correct operation of each service, ensuring that the infrastructure meets the security and functionality requirements [7].*

KEYWORDS: GNU/Linux, NethServer, Virtualization, Network Security, Local Area Network, DHCP Server, DNS Server, Domain Controller, Web Proxy, Firewall, File Server, Print Server, VPN

1 INTRODUCCIÓN

La creciente complejidad de las redes informáticas modernas exige soluciones robustas y flexibles para la gestión de servicios de red e infraestructura IT. Las pequeñas y medianas empresas (PyMEs) requieren soluciones que les permitan administrar eficientemente sus recursos, garantizar la seguridad de la información y facilitar el acceso remoto a sus redes. En este contexto, las distribuciones GNU/Linux especializadas en la gestión de servidores, como NethServer, se presentan como una alternativa atractiva frente a soluciones propietarias.

NethServer, una distribución de código abierto basada en CentOS, ofrece una amplia gama de funcionalidades para la administración de redes, incluyendo servidor DHCP, servidor DNS, controlador de dominio, firewall, proxy web, servidor de archivos, servidor de impresión y VPN. Su interfaz intuitiva y su amplio conjunto de herramientas facilitan la configuración y el mantenimiento de la infraestructura de red.

Este artículo describe la implementación paso a paso de un servidor GNU/Linux utilizando la distribución NethServer 7.9.2009 en una máquina virtual. El objetivo principal es construir una infraestructura de red completa que satisfaga las necesidades de una PyME típica, incluyendo la gestión de usuarios, el acceso a recursos compartidos, la seguridad perimetral y el acceso remoto seguro. Se detallarán los pasos necesarios para la configuración de cada servicio, así como las pruebas de validación realizadas para asegurar su correcto funcionamiento.

2 INSTALACIÓN DE NETHSERVER

2.1 REQUERIMIENTOS MÍNIMOS

Los requisitos básicos para el funcionamiento de NethServer son:

- CPU de 64 bits (x86_64)
- 1 GB de RAM
- 10 GB de espacio en disco
- Interfaz de red

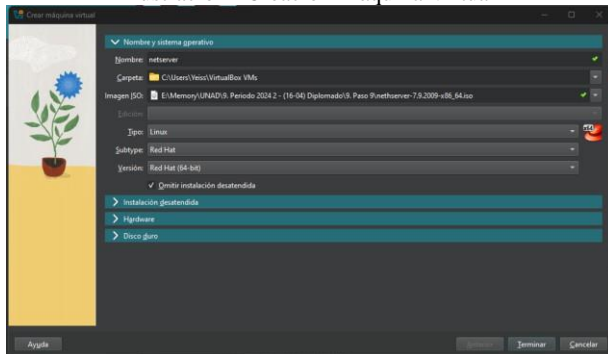
2.2 ENLACE DE DESCARGA

<https://github.com/NethServer/dev/releases/tag/iso-7.9.2009>

2.3 PROCESO DE INSTALACIÓN

Luego de realizar la descarga de la imagen ISO, se procede a determinar los recursos necesarios para la instalación y el funcionamiento de NethServer [1].

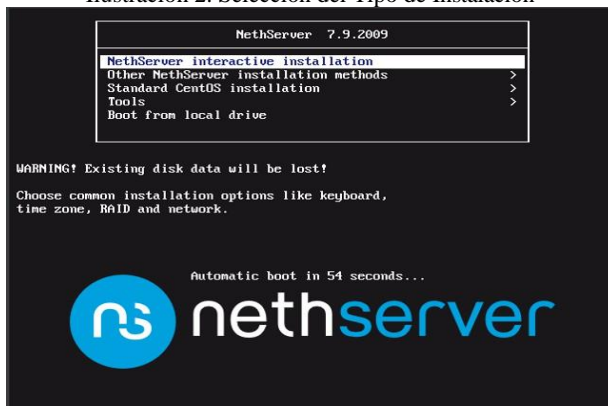
Ilustración 1 Creación Máquina Virtual



Fuente: Autoría Propia

Al finalizar la configuración de la máquina virtual, se debe iniciar el proceso de instalación.

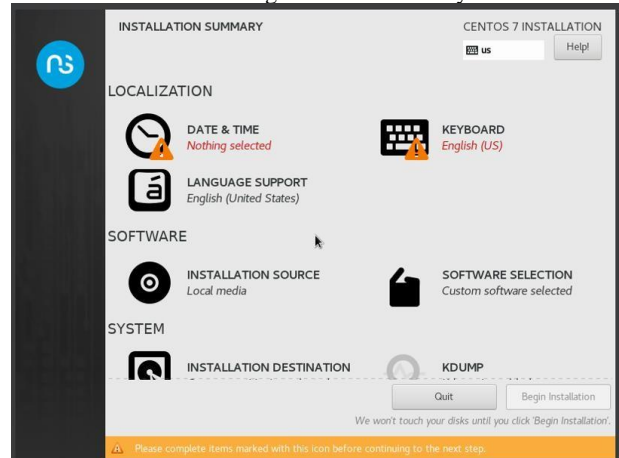
Ilustración 2. Selección del Tipo de Instalación



Fuente: Autoría Propia

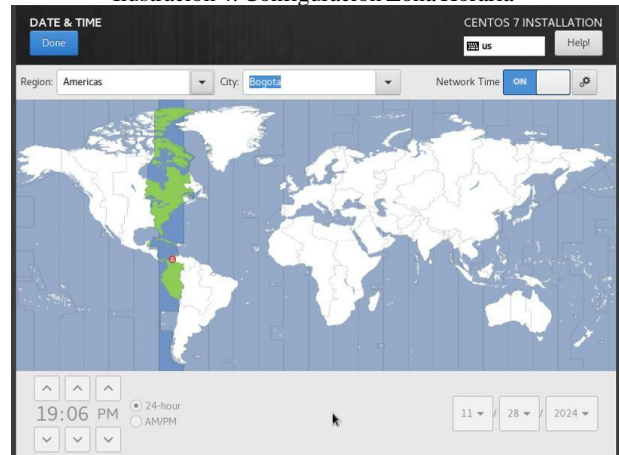
Luego de finalizar la copia de archivos de la imagen ISO, se requiere establecer la configuración de la zona horaria y la distribución del teclado, según se describe en la documentación oficial de NethServer [8].

Ilustración 3. Configurar Zona Horaria y Teclado



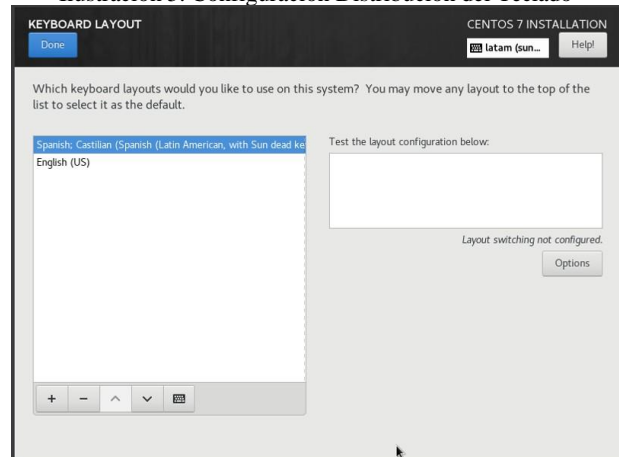
Fuente: Autoría Propia

Ilustración 4. Configuración Zona Horaria



Fuente: Autoría Propia

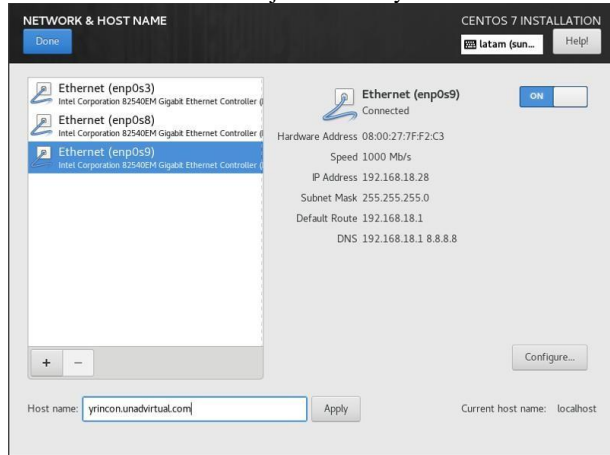
Ilustración 5. Configuración Distribución del Teclado



Fuente: Autoría Propia

En las opciones de red y de host name, verificamos que las tarjetas de red se encuentren disponibles y se asigna un nombre de dominio.

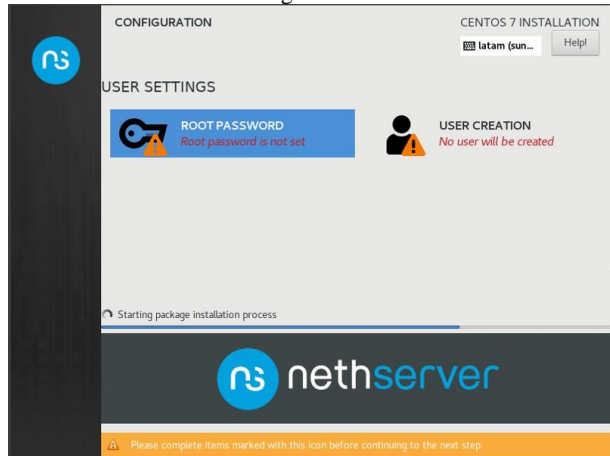
Ilustración 6. Tarjetas de Red y Host Name



Fuente: Autoría Propia

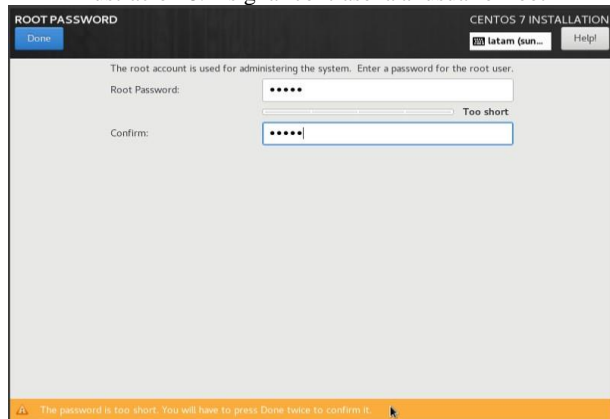
Es necesario asignar una contraseña al usuario Root.

Ilustración 7. Configuración del usuario Root



Fuente: Autoría Propia

Ilustración 8. Asignar contraseña al usuario Root



Fuente: Autoría Propia

Al finalizar la instalación del NethServer se visualiza la dirección IP y el puerto al que se puede acceder desde la interfaz web.

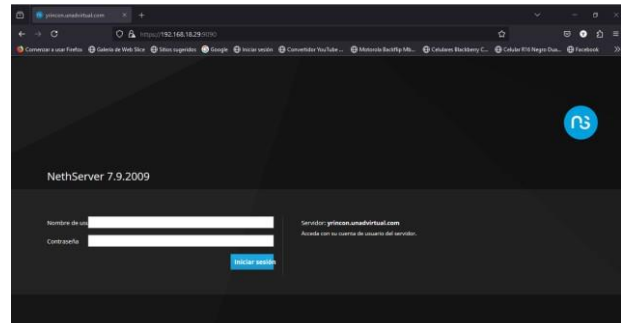
Ilustración 9. Asignar contraseña al usuario Root



Fuente: Autoría Propia

Al finalizar la instalación del NethServer se visualiza la dirección IP y el puerto al que se puede acceder desde la interfaz web.

Ilustración 10. Interfaz Web NethServer



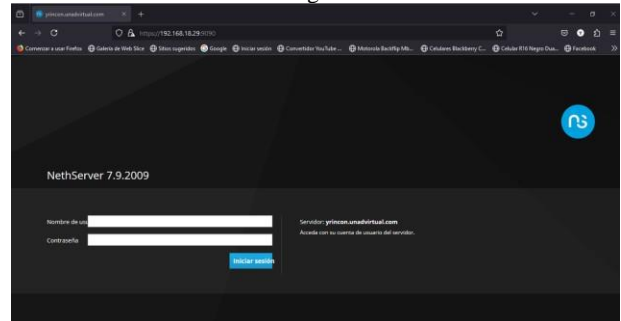
Fuente: Autoría Propia

3 DESARROLLO DE TEMÁTICAS

3.1 DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de infraestructura IT de NethServer.

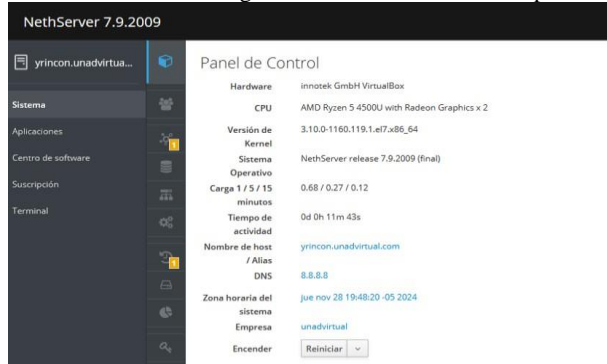
Ilustración 11. Ingreso a NethServer



Fuente: Autoría Propia

Se inicia la configuración de las diferentes redes que se van a utilizar en las conexiones de los dispositivos.

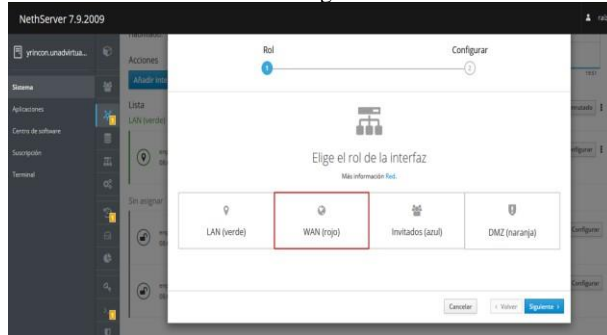
Ilustración 12. Configuración del Nombre de la Empresa



Fuente: Autoría Propia

Se procede a configurar la red WAN (Zona ROJA) la cual va a representar el acceso a internet.

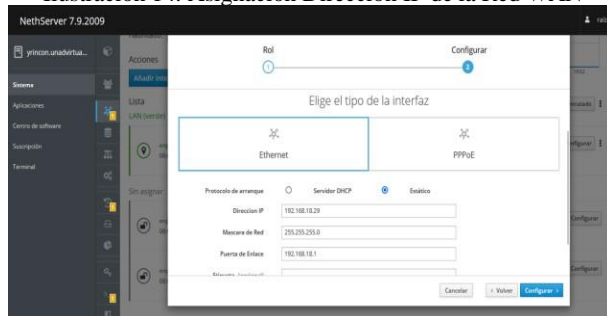
Ilustración 13. Configuración red WAN



Fuente: Autoría Propia

Se asigna una dirección IP, este procedimiento es necesario para que la MV no cambie la dirección IP automáticamente cada vez que se reinicie.

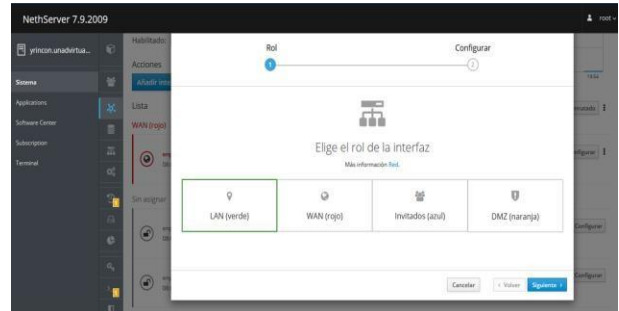
Ilustración 14. Asignación Dirección IP de la Red WAN



Fuente: Autoría Propia

Se continúa con la configuración de la red LAN (Zona VERDE).

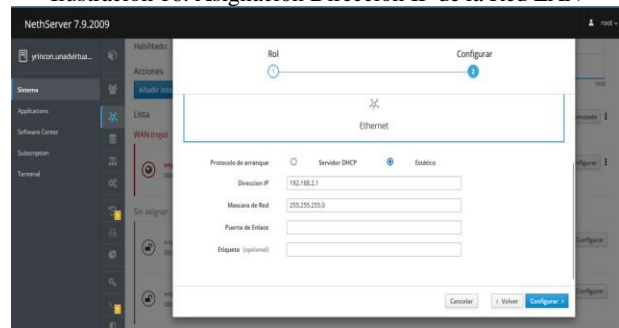
Ilustración 15. Configuración de la red LAN



Fuente: Autoría Propia

Se asigna una dirección IP diferente para evitar conflictos entre las redes.

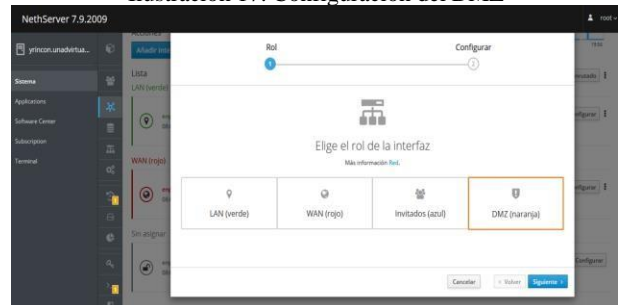
Ilustración 16. Asignación Dirección IP de la Red LAN



Fuente: Autoría Propia

Se continúa con la configuración del (Zona NARANJA).

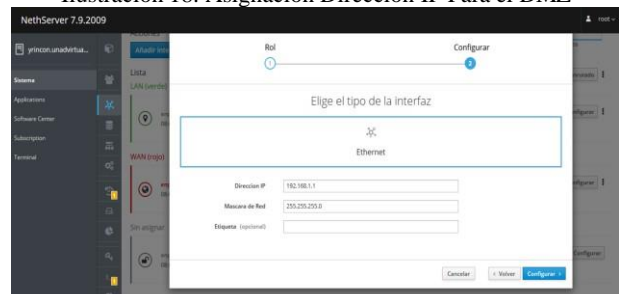
Ilustración 17. Configuración del DMZ



Fuente: Autoría Propia

Se asigna una dirección IP diferente para evitar conflictos entre las redes.

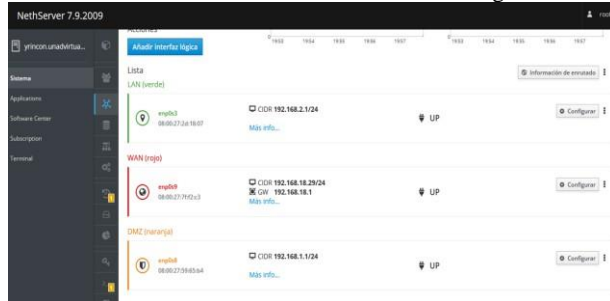
Ilustración 18. Asignación Dirección IP Para el DMZ



Fuente: Autoría Propia

Se verifica la configuración de las redes y se valida que cumplan con los requerimientos.

Ilustración 19. Validación de las Redes Configuradas

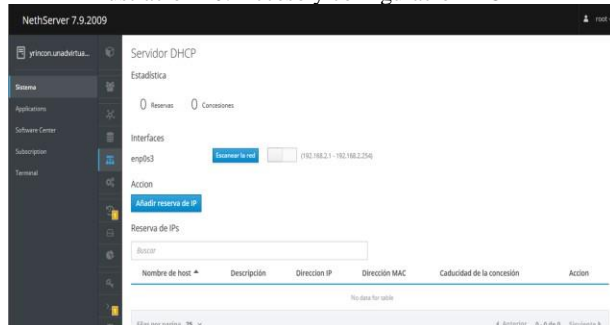


Fuente: Autoría Propia

3.1.1 DHCP Server

Se ingresa al panel de navegación izquierdo y seleccionamos la opción (Servidor DHCP) para configurar el rango de direcciones IP disponible, de acuerdo con la guía de administración de NethServer [3].

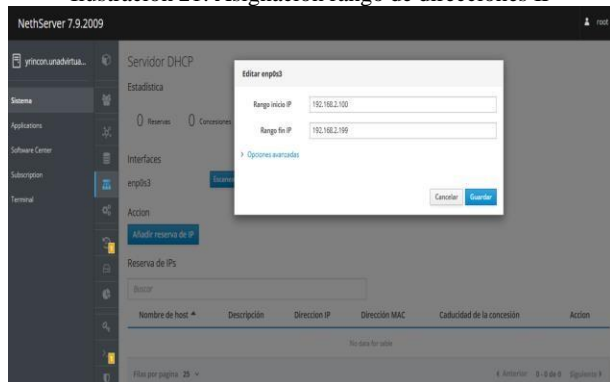
Ilustración 20. Acceso y configuración DHCP



Fuente: Autoría Propia

Se asigna el rango de direcciones IP que van a estar disponibles para la MV.

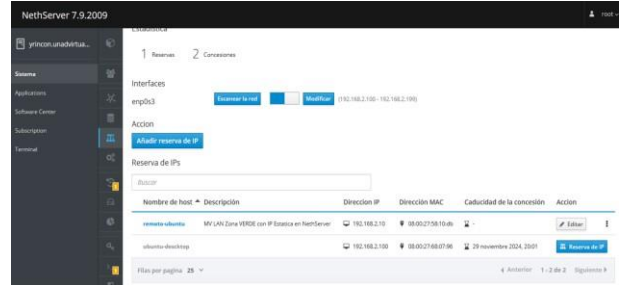
Ilustración 21. Asignación rango de direcciones IP



Fuente: Autoría Propia

Una vez configurado el rango de las direcciones IP y luego de haber añadido las direcciones IP de reserva, se verifica que la información se haya realizado de forma correcta.

Ilustración 22. Validación funcionamiento del DHCP

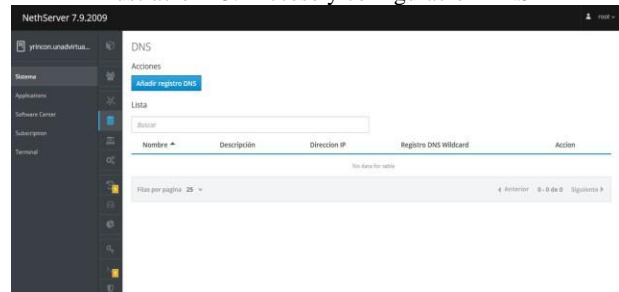


Fuente: Autoría Propia

3.1.2 DNS Server y Controlador de Dominio

Se ingresa al panel de navegación izquierdo y seleccionamos la opción (Servidor DNS).

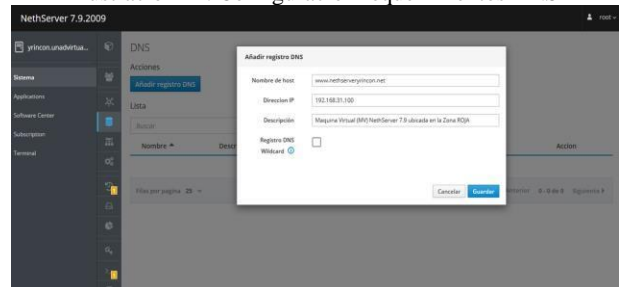
Ilustración 23. Acceso y configuración DNS



Fuente: Autoría Propia

Se realiza la configuración del servidor DNS estableciendo los requerimientos necesarios para su funcionamiento.

Ilustración 24. Configuración requerimientos DNS



Fuente: Autoría Propia

Una vez realizada la configuración, se verifica que el DNS esté en funcionamiento.

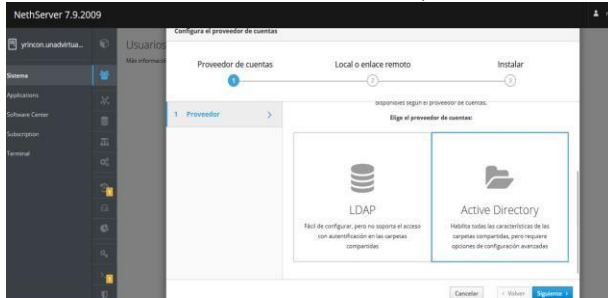
Ilustración 25. Validación funcionamiento del DNS



Fuente: Autoría Propia

A continuación, se inicia la creación del usuario de dominio por medio de la herramienta (SAMBA ACTIVE DIRECTORY).

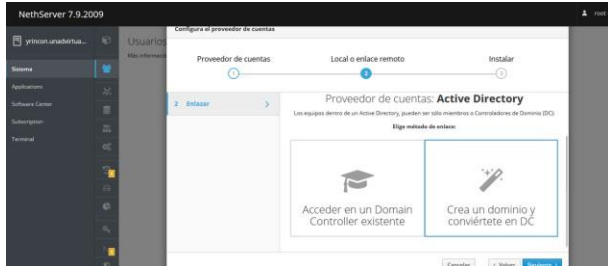
Ilustración 26. Configuración e instalación de (SAMBA ACTIVE DIRECTORY)



Fuente: Autoría Propia

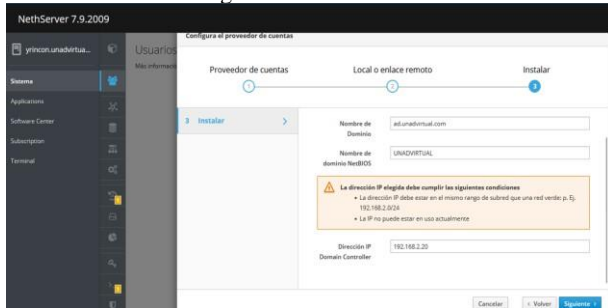
Se continúa con la creación del dominio, para este caso se utiliza la herramienta (CREAR UN DOMINIO EN DC)

Ilustración 27. Creación del Dominio



Fuente: Autoría Propia

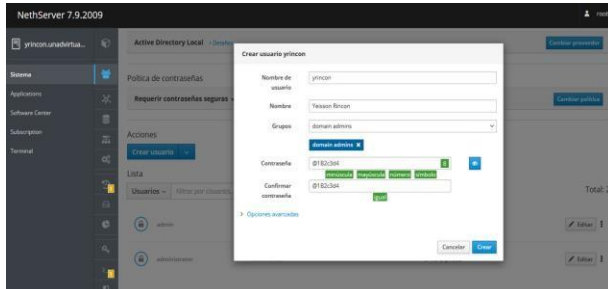
Ilustración 28. Configuración de la información del dominio



Fuente: Autoría Propia

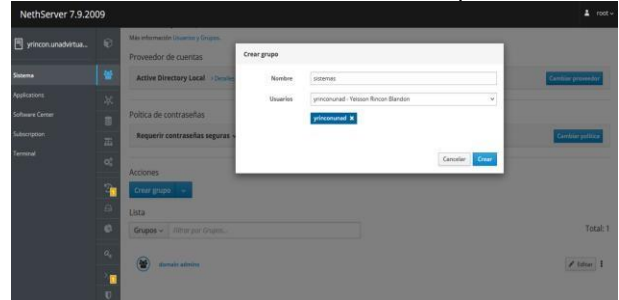
Se crean los usuarios y grupos que van a tener acceso a nuestra red.

Ilustración 29. Creación del usuario



Fuente: Autoría Propia

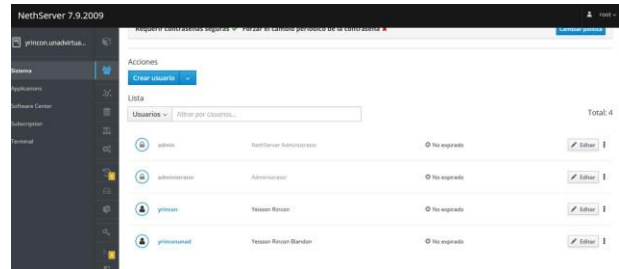
Ilustración 30. Creación del Grupo



Fuente: Autoría Propia

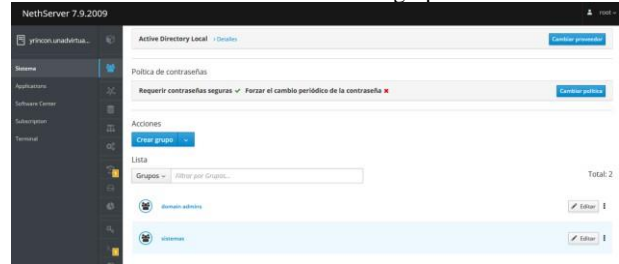
Una vez creado el usuario y el grupo, se valida que el sistema haya tomado la información de forma correcta.

Ilustración 31. Validación del usuario creado



Fuente: Autoría Propia

Ilustración 32. Validación del grupo creado



Fuente: Autoría Propia

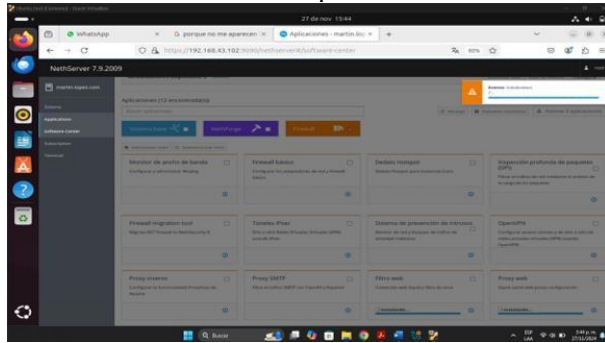
3.2 PROXY WEB

El proxy web es un servicio que se encuentra entre Hosts de una misma o diferentes LAN y los sitios de Internet, como se detalla en [6]. Donde se puede tener control de navegación y reducción de uso del ancho de banda mediante el almacenamiento en cache de las páginas web comúnmente visitada.

3.2.1 Instalación del servicio

En el menú ubicado sobre el lado inferior izquierdo, nos dirigimos a Software Center e instalamos las aplicaciones "Web Proxy" y "Filtro Web".

Ilustración 33. Selección de aplicaciones a instalar.

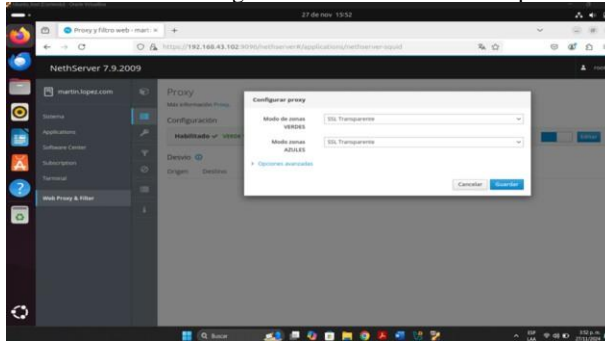


Fuente: Autoría Propia

3.2.2 Configuración de proxy

Se habilita el Proxy en modo SSL Transparente en la zona verde.

Ilustración 34. Configuración del modo SSL Transparente

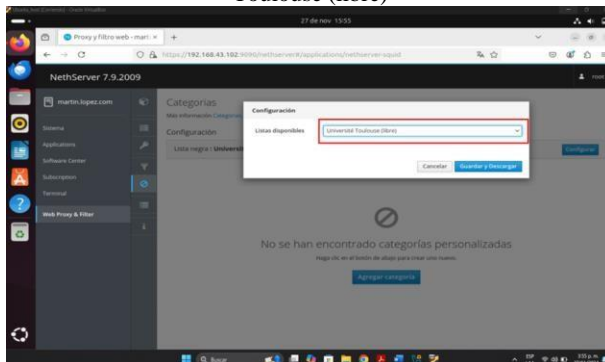


Fuente: Autoría Propia

Categorías de Filtrado:

- Se descarga la lista "Universite Toulouse (libre)".
- Se bloquea categorías no deseadas (e.g., redes sociales).

Ilustración 35. Guardado y descarga de la lista Universite Toulouse (libre)



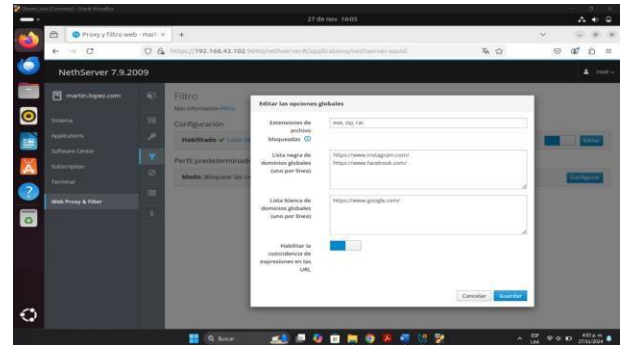
Fuente: Autoría Propia

3.2.3 Configuración de políticas

Listas Negra y Blanca

- Se agrega dominios bloqueados como facebook.com e instagram.com a la lista negra.
- Se autoriza sitios como google.com en la lista blanca.

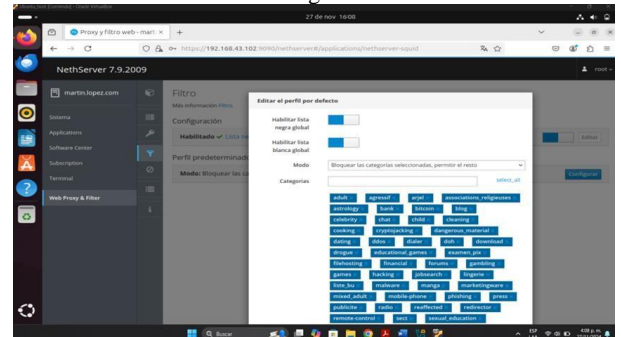
Ilustración 36. Configuración del filtro en las listas negra y blanca



Fuente: Autoría Propia

Se procede a configurar las categorías de filtro, lo que nos permite controlar el acceso a sitios no deseados. Estas categorías pueden seleccionarse según nuestras necesidades. Una vez configuradas, garantizan una navegación más segura y eficiente.

Ilustración 37. Configuración de categorías de filtrado para la navegación

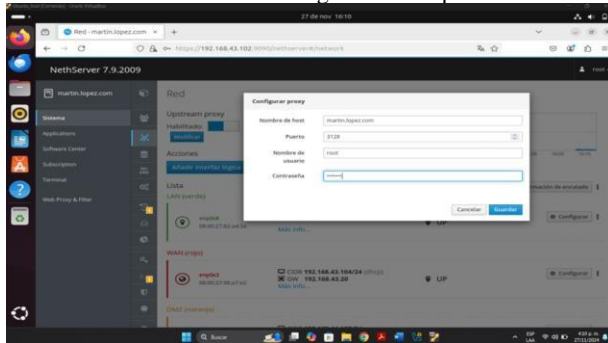


Fuente: Autoría Propia

3.2.4 Habilitación del proxy en la sección Red

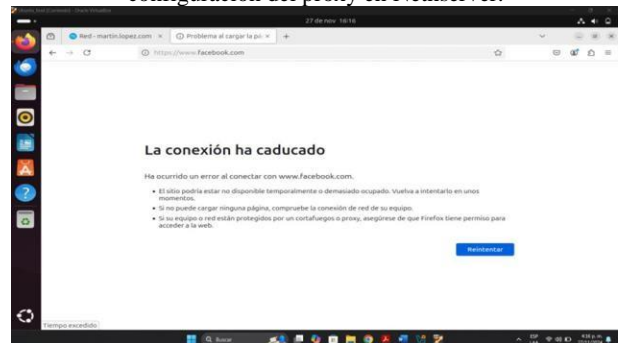
Se configura el puerto del Proxy en 3128 a través de las opciones de la sección red de Nethserver.

Ilustración 38. Configuración del puerto



Fuente: Autoría Propia

Ilustración 40. Rechazo de acceso a Facebook tras configuración del proxy en Nethserver.



Fuente: Autoría Propia

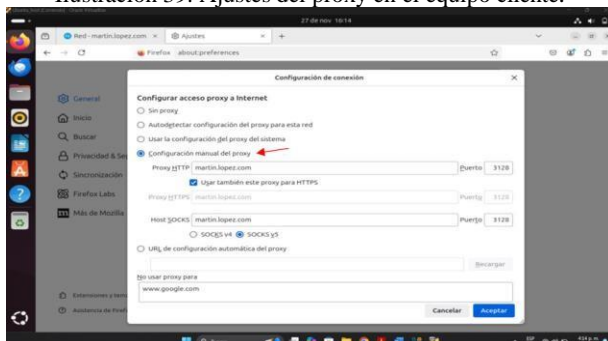
3.2.5 Configuración en el cliente

En la configuración manual del proxy, se puede especificar un servidor proxy para HTTP y HTTPS indicando su dirección y puerto. Además, se puede habilitar un host SOCKS, eligiendo entre SOCKS v4 o v5. Existe la opción de excluir ciertos sitios, como www.google.com, del uso del proxy. Esta configuración permite personalizar cómo se enrutan las conexiones de red a través del proxy especificado.

Configura manualmente el Proxy en el navegador del equipo cliente:

- **Dirección del Proxy:** http://[IP-servidor o dominio]:3128.
- **Excepciones:** Añade sitios permitidos en la configuración.

Ilustración 39. Ajustes del proxy en el equipo cliente.

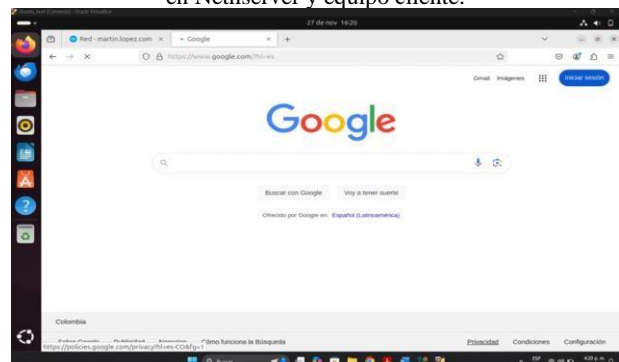


Fuente: Autoría Propia

Gestión Centralizada:

- La interfaz de NethServer facilitó la administración y monitoreo de políticas en tiempo real.

Ilustración 41. Acceso a Google tras configuración del proxy en Nethserver y equipo cliente.



Fuente: Autoría Propia

3.3 CONFIGURACION FILE SERVER Y PRINT SERVER

Un **File Server** (servidor de archivos) es un sistema que proporciona un espacio centralizado para almacenar y compartir archivos en una red. Utiliza protocolos como SMB (Server Message Block) o NFS (Network File System) para facilitar el acceso remoto de usuarios y dispositivos. Este servicio permite a las organizaciones:

- Almacenar datos de forma segura.
- Gestionar accesos y permisos de usuarios mediante autenticación.
- Mejorar la colaboración al compartir archivos de manera controlada.

En el caso de NethServer, se utiliza Samba para gestionar el File Server, lo que permite compartir recursos entre sistemas Windows y Linux de manera eficiente y segura.

Un **Print Server** (servidor de impresión) es un sistema que administra la conexión y el acceso a impresoras en una red. Este servicio centraliza las tareas de impresión, permitiendo:

3.2.6 Resultado

Control de Tráfico:

- Se logró bloquear sitios como facebook.com, mientras se permitía el acceso a google.com.

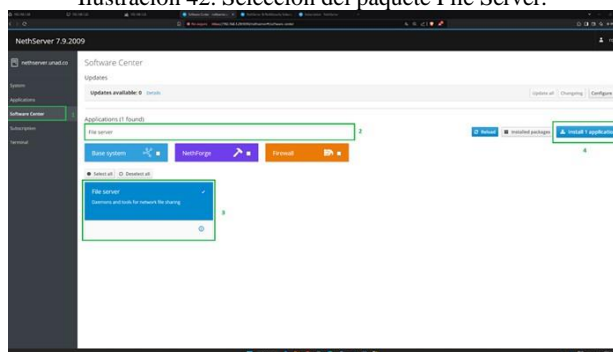
- Configurar y gestionar múltiples impresoras desde un único punto.
- Monitorizar y controlar trabajos de impresión.
- Optimizar el uso de impresoras en entornos empresariales.

NethServer utiliza el servicio CUPS (Common UNIX Printing System) para gestionar el Print Server, proporcionando una interfaz intuitiva para la administración de impresoras locales y en red.

3.3.1 Instalación del servicio

La instalación del servicio de File Server en NethServer centraliza la gestión de archivos, permitiendo un acceso eficiente y seguro a los recursos compartidos en una red empresarial. Utilizando Samba, el sistema garantiza interoperabilidad entre plataformas Windows y Linux, reduciendo los problemas de compatibilidad. Este módulo se habilita desde el Software Center de NethServer seleccionando el paquete "File Server".

Ilustración 42. Selección del paquete File Server.

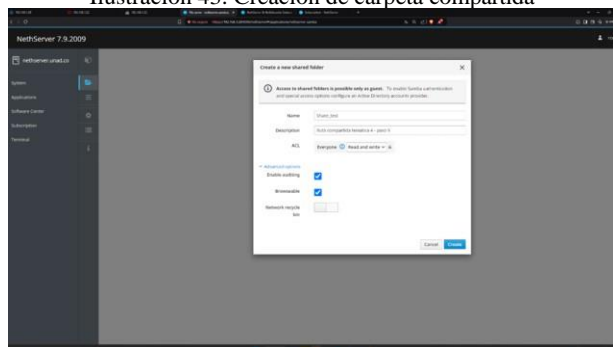


Fuente: Autoría Propia

3.3.2 Configuración de Carpetas Compartidas

La creación de carpetas compartidas permite a los usuarios de la red acceder a archivos de manera controlada, optimizando la colaboración y reduciendo redundancias en el almacenamiento de datos, según se describe en la documentación oficial [2]. Se puede configurar desde el módulo "Shared Folders", donde se define el nombre de la carpeta, los permisos de acceso, y se asignan políticas de auditoría.

Ilustración 43. Creación de carpeta compartida

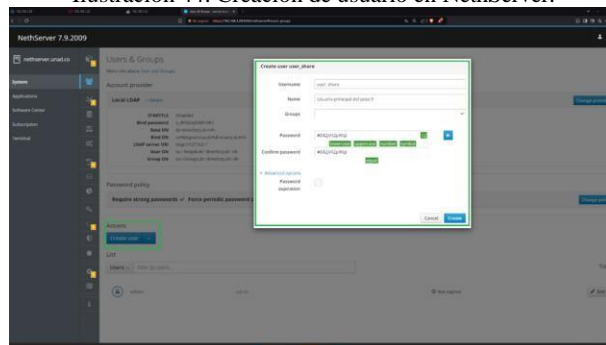


Fuente: Autoría Propia

3.3.3 Gestión de Usuarios

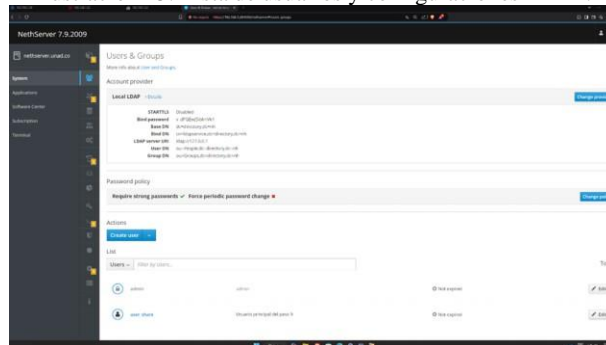
La administración de usuarios asegura que solo personas autorizadas accedan a los recursos compartidos, fortaleciendo la seguridad de los datos. Se configura un proveedor de cuentas LDAP en el módulo "Accounts Provider" de NethServer y se crean usuarios con permisos específicos para acceder a las carpetas compartidas.

Ilustración 44. Creación de usuario en NethServer.



Fuente: Autoría Propia

Ilustración 45. Lista de usuarios y configuraciones LDAP.



Fuente: Autoría Propia

3.3.4 Validación de Acceso desde Cliente Linux

Para asegurar la funcionalidad del servicio de File Server, se realizó una prueba de acceso desde un cliente Linux. En primer lugar, se instalaron las herramientas necesarias para la interacción con el servidor, como **cifs-utils** y **smbclient**. Una vez instaladas, se configuró el montaje de la carpeta compartida. A continuación, se verificó que los usuarios definidos en el servidor pudieran acceder a los recursos con las credenciales asignadas.

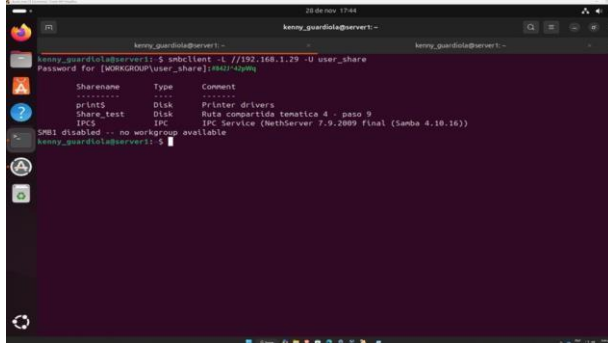
El comando utilizado para montar la carpeta compartida fue:

```
sudo mount -t cifs //IP-servidor/Compartida /mnt/carpeta -o user=user1
```

La carpeta se montó correctamente en el directorio /mnt/carpeta, y se validó la lectura y escritura de archivos dentro de la carpeta compartida por parte del usuario autenticado. Asimismo, se comprobó que los permisos

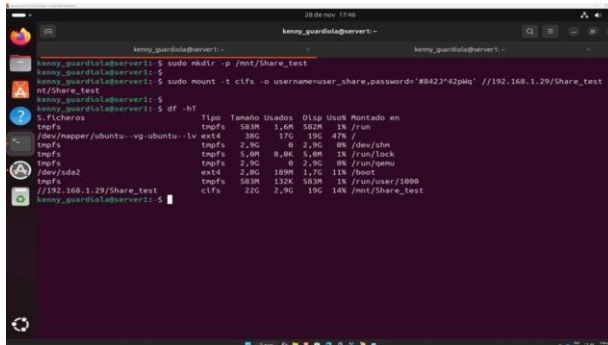
configurados en el servidor respetaran las restricciones de acceso para usuarios no autorizados.

Ilustración 46. Verificación de recursos compartidos en la red.



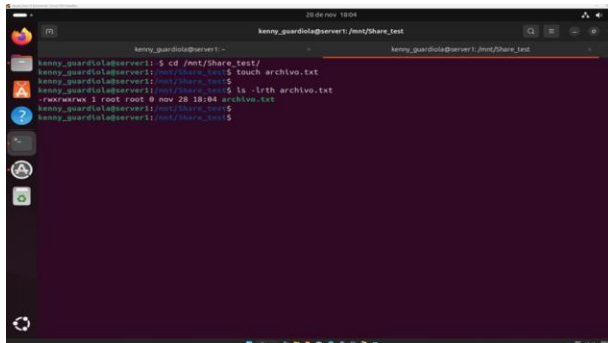
Fuente: Autoría Propia

Ilustración 47. Montaje de un recurso compartido en el sistema local.



Fuente: Autoría Propia

Ilustración 48. Acceso exitoso a la carpeta compartida desde cliente Linux.



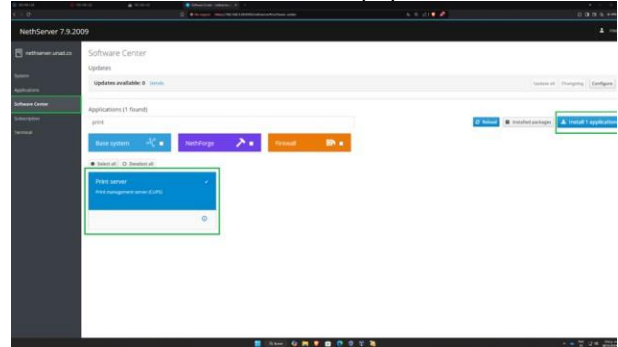
Fuente: Autoría Propia

Esta validación confirmó la correcta configuración y operatividad del File Server, garantizando que los recursos compartidos estuvieran disponibles y protegidos conforme a las políticas establecidas.

3.3.5 Instalación del Print Server

La habilitación del Print Server mediante CUPS en NethServer centraliza la administración de impresoras, permitiendo configurar, monitorear y gestionar trabajos de impresión de manera eficiente [5]. Se instala desde el Software Center seleccionando el paquete "Print Server (CUPS)".

Ilustración 49. Instalación del paquete Print Server.



Fuente: Autoría Propia

3.3.5 Configuración de impresoras

La configuración de impresoras en el Print Server de NethServer se realiza a través del sistema CUPS, permitiendo gestionar dispositivos de impresión de manera centralizada. Este proceso asegura que los recursos de impresión estén accesibles y controlados en toda la red, optimizando la administración de tareas de impresión en entornos empresariales o educativos.

Inicialmente, se accede al módulo de administración de impresoras en la interfaz gráfica de NethServer. Desde esta sección, se puede agregar una nueva impresora virtual o física, dependiendo de las necesidades de la red. En este caso, se configuró una impresora virtual (PDF Printer) para pruebas funcionales.

Se definieron los parámetros de la impresora, incluyendo:

- **Nombre:** PDFPrinter.
- **Compartición en red:** Habilitada para usuarios autenticados.
- **Protocolo de conexión:** IPP (Internet Printing Protocol).

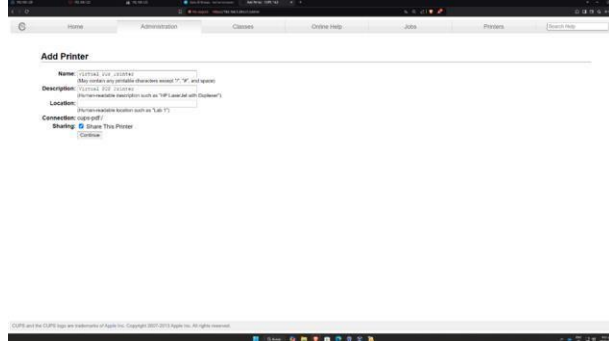
Una vez configurada, se realizó una validación para asegurar que la impresora estuviera disponible en la red. Este paso incluyó la verificación de la conectividad desde clientes Linux, donde se comprobó la correcta detección del dispositivo y su disponibilidad para tareas de impresión.

Ilustración 50. Adición de una impresora virtual en CUPS.



Fuente: Autoría Propia

Ilustración 51. Configuración de impresora virtual en CUPS.



Fuente: Autoría Propia

Con esta configuración, el Print Server queda listo para gestionar dispositivos de impresión, ya sean virtuales o físicos, asegurando una solución flexible y escalable para los usuarios de la red.

3.3.6 Validación de Impresión desde Cliente Linux

La validación de impresión desde un cliente Linux asegura la operatividad y funcionalidad del Print Server configurado en NethServer. Este paso es fundamental para verificar que la impresora esté correctamente compartida y accesible desde dispositivos conectados a la red.

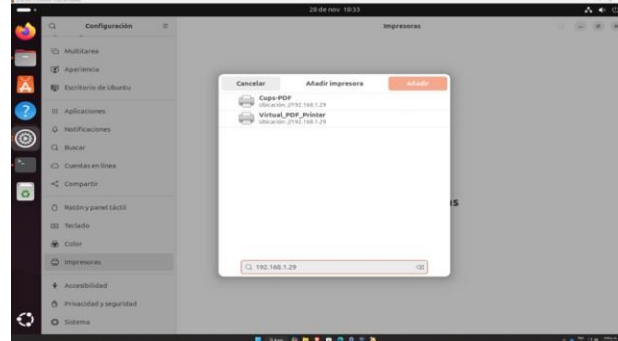
Inicialmente, se accedió al menú de configuración de impresoras en el cliente Linux. Desde la opción de "Configuración de Impresoras", se seleccionó "Añadir Impresora". En el asistente de configuración, se eligió la impresora compartida en el servidor, identificada por su nombre (PDFPrinter) y el protocolo IPP.

Durante el proceso de configuración, se definieron los siguientes parámetros, siguiendo las recomendaciones descritas en la documentación de CUPS en NethServer [5]:

- **Protocolo de Conexión:** IPP (Internet Printing Protocol).
- **Dirección del Servidor:** `ipp://IP-servidor/printers/PDFPrinter`.
- **Opciones de Impresión:** Ajustadas según las necesidades de prueba.

Una vez finalizada la configuración, se realizó una prueba de impresión desde la interfaz gráfica del cliente. Se utilizó un archivo de texto simple para confirmar que el trabajo de impresión fuera enviado correctamente al Print Server de NethServer. Tras procesar el trabajo, la impresora virtual (PDFPrinter) generó un archivo PDF como resultado.

Ilustración 52. Configuración de la impresora en cliente Linux.



Fuente: Autoría Propia

La prueba confirmó que la comunicación entre el cliente y el servidor era estable y que el trabajo de impresión se procesó sin inconvenientes. Esto valida la operatividad del servicio de impresión en la red, garantizando que los usuarios puedan utilizar las impresoras configuradas sin dificultades técnicas.

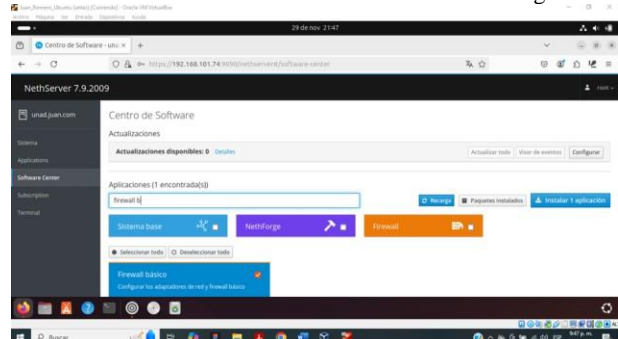
3.4 CORTAFUEGOS (FIREWALL)

La instalación y configuración del cortafuegos en NethServer es fundamental para controlar el tráfico de red y garantizar la seguridad en el acceso a recursos internos y externos. Este proceso asegura que las políticas de restricción se implementen de manera efectiva, utilizando las reglas definidas en la documentación del firewall de NethServer [4].

3.4.1 Proceso de Instalación

- Desde el panel de administración de NethServer, se accedió al Software Center.
- Se seleccionó e instaló el módulo Firewall Básico, que permite configurar reglas personalizadas para el tráfico de red.

Ilustración 53. Instalación del módulo de cortafuegos.



Fuente: Autoría Propia

Una vez instalado, el firewall queda disponible en el panel de control para proceder con las configuraciones avanzadas.

3.4.2 Configuración del firewall de Instalación

Después de la instalación, se configuraron las reglas necesarias para bloquear sitios de entretenimiento, como Facebook e Instagram. Antes de la configuración, se realizaron

pruebas de conectividad para identificar las direcciones IP de los sitios web mediante comandos ping. Esto garantiza la precisión de las reglas.

En el módulo del firewall, se crearon dos reglas principales:

- **Regla 1:** Bloqueo del acceso a Facebook mediante HTTPS.
- **Regla 2:** Bloqueo del acceso a Instagram mediante HTTPS.

Detalles de las reglas:

- **Protocolo:** HTTPS.
- **Destino:** las direcciones IP de Instagram y de Facebook
- **Acción:** Denegar el acceso.

Las reglas fueron aplicadas sobre la interfaz correspondiente (e.g., LAN), y se habilitaron de inmediato para que los cambios surtieran efecto.



Ilustración 54. Panel de control del firewall.

Fuente: Autoría Propia

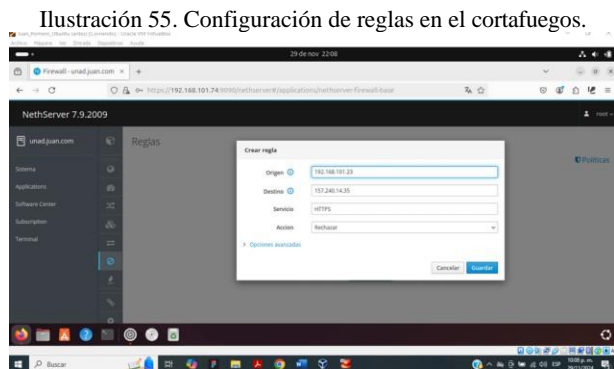
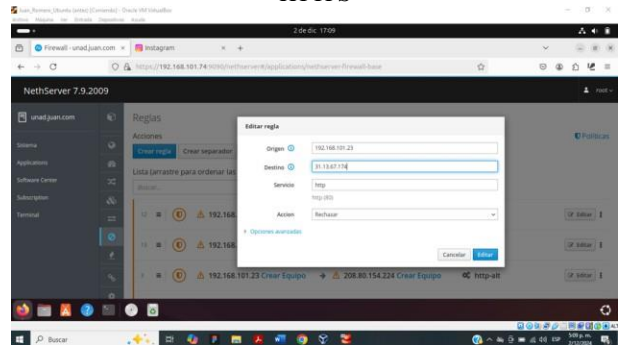


Ilustración 55. Configuración de reglas en el cortafuegos.

Fuente: Autoría Propia

Ilustración 56. Configuración de la regla para Instagram por HTTPS



Fuente: Autoría Propia

El cortafuegos comenzó a filtrar el tráfico de acuerdo con las reglas establecidas, asegurando que el acceso no autorizado fuera bloqueado.

3.4.2 Validación del firewall

La validación del cortafuegos configurado en NetServer asegura que las reglas de seguridad implementadas funcionen correctamente, restringiendo el acceso a los sitios web especificados y garantizando el cumplimiento de las políticas de red. Este proceso incluyó la comprobación de conectividad inicial y la verificación de las restricciones tras la implementación de las reglas.

Inicialmente, se verificó que los sitios objetivo, Facebook e Instagram, fueran accesibles desde un cliente Linux. Esto se realizó utilizando un navegador web, confirmando que no existían restricciones previas. Además, mediante el comando ping, se identificaron las direcciones IP asociadas a estos dominios, información que sirvió para definir las reglas de bloqueo en el cortafuegos.

Una vez configuradas las reglas en el firewall, se intentó acceder nuevamente a los sitios desde el cliente. Ambos intentos fueron rechazados, lo que confirmó que las restricciones eran efectivas. En el navegador, los usuarios recibieron mensajes de error al intentar cargar las páginas de los sitios bloqueados. Adicionalmente, se revisó el registro del firewall para verificar que las solicitudes fueron filtradas correctamente.

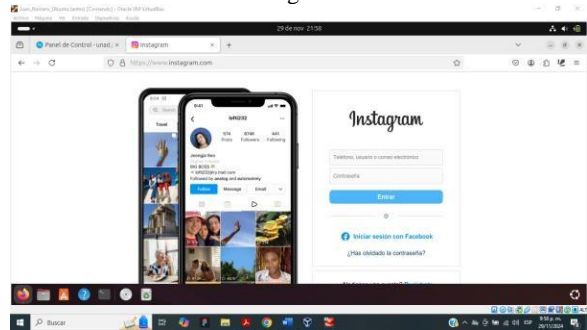
Por último, se realizaron pruebas adicionales para comprobar que los sitios no bloqueados permanecían accesibles, asegurando que las restricciones no afectaran otros dominios o servicios autorizados en la red.

Ilustración 57. Acceso inicial a Facebook antes de aplicar las reglas.



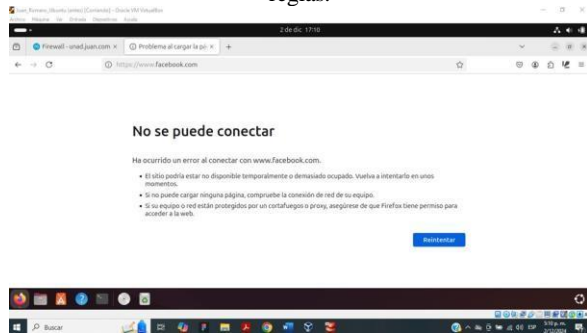
Fuente: Autoría Propia

Ilustración 58. Acceso inicial a Instagram antes de aplicar las reglas.



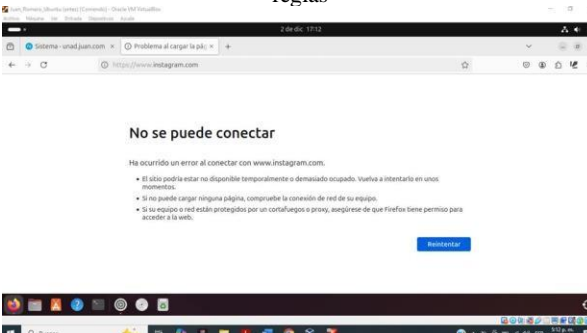
Fuente: Autoría Propia

Ilustración 59. Bloqueo de acceso a Facebook tras aplicar las reglas.



Fuente: Autoría Propia

Ilustración 60. Bloqueo de acceso a Instagram tras aplicar las reglas.



Fuente: Autoría Propia

La validación demostró que el cortafuegos configurado en NethServer bloqueó eficazmente el tráfico hacia los sitios no autorizados, reforzando las medidas de seguridad y control en la red interna. Este resultado confirma que las reglas definidas cumplen con los objetivos establecidos para proteger los recursos de la red.

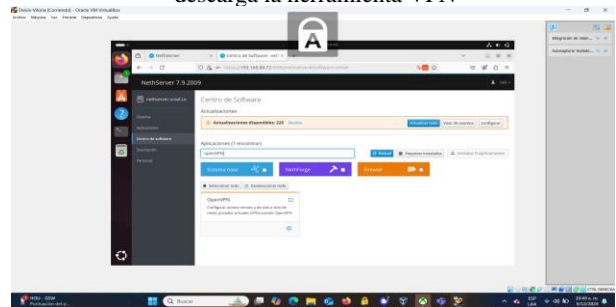
3.5 VPN (VIRTUAL PRIVATE NETWORK)

La instalación y configuración de una VPN (Virtual Private Network) en NethServer es esencial para garantizar conexiones seguras entre dispositivos remotos y la red corporativa. Este servicio permite crear un túnel encriptado que protege la transmisión de datos, asegurando privacidad y acceso seguro a recursos internos desde ubicaciones externas [7].

3.5.1 Instalación del servicio

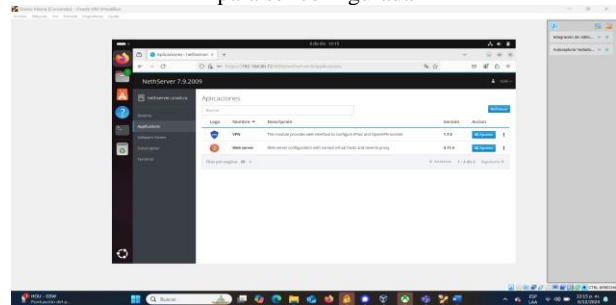
El módulo de VPN fue instalado desde el Software Center de NethServer, utilizando la herramienta OpenVPN. Este proceso incluyó la creación de usuarios específicos y la generación de certificados de seguridad necesarios para autenticar las conexiones remotas. La implementación sigue las recomendaciones oficiales de NethServer, garantizando que las conexiones sean confiables y seguras [7].

Ilustración 61. En el centro de Software de Nethserver se descarga la herramienta VPN



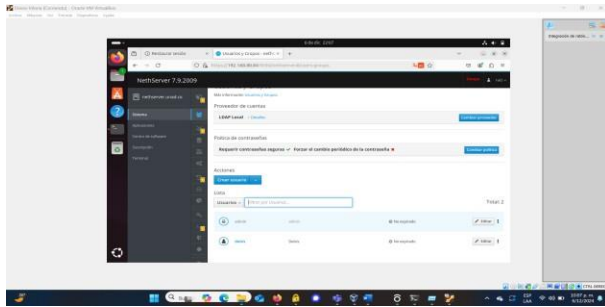
Fuente: Autoría Propia

Ilustración 62. Se evidencia la aplicación VPN instalada y lista para ser configurada



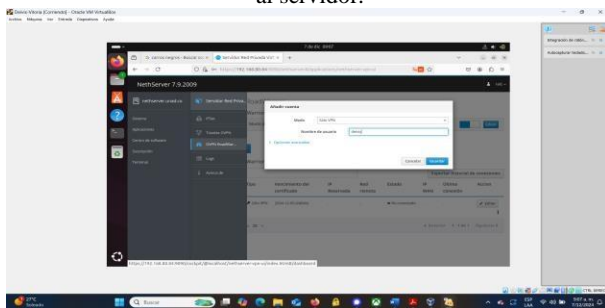
Fuente: Autoría Propia

Ilustración 63. Se crea el usuario con el que vamos a establecer el certificado de conexión en la VPN



Fuente: Autoría Propia

Ilustración 64. Se añade la cuenta creada al del OpenVPN RoadWarriors para establecer la conexión desde un dispositivo al servidor.



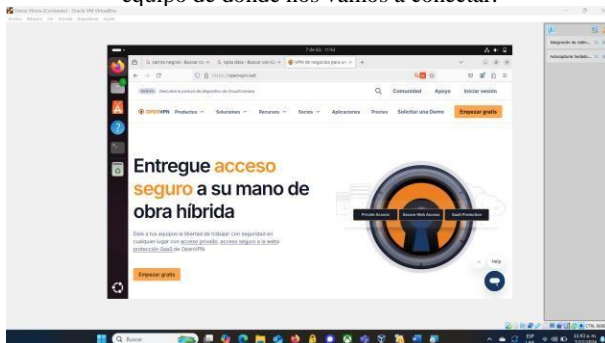
Fuente: Autoría Propia

3.5.2 Configuración de la app de VPN

En el equipo remoto, se descargó e instaló la aplicación OpenVPN. Se configuraron las credenciales del usuario y se importó el certificado emitido por el servidor. El cliente fue parametrizado con los siguientes datos:

- **Protocolo:** OpenVPN UDP/TCP.
- **Servidor:** Dirección IP o dominio del servidor NethServer.
- **Certificado:** Emitido por el servidor para garantizar la autenticidad de la conexión.

Ilustración 65. Se procede a descargar el ejecutable en el equipo de donde nos vamos a conectar.

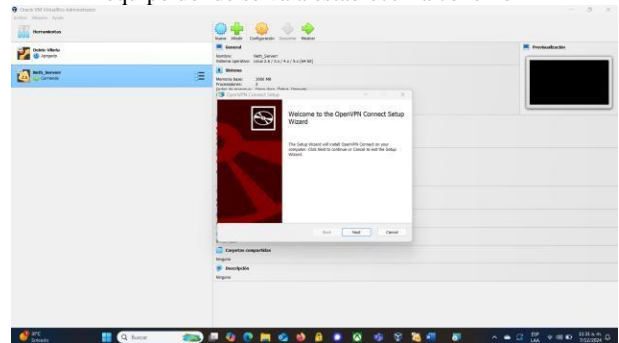


Fuente: Autoría Propia

Las pruebas realizadas confirmaron que la conexión entre el cliente y el servidor era estable y que el tráfico estaba

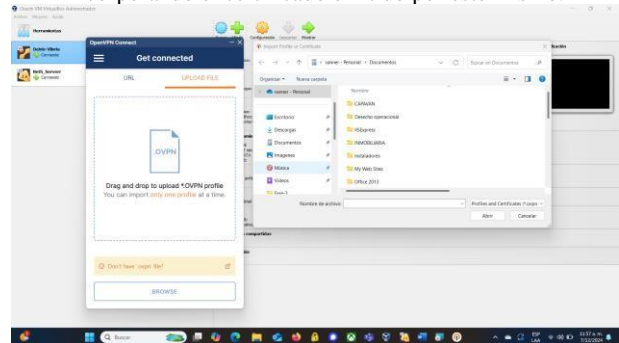
completamente cifrado, asegurando protección contra accesos no autorizados [7].

Ilustración 66. Se instala el ejecutable de OpenVpn en el equipo donde se va a establecer la conexión



Fuente: Autoría Propia

Ilustración 67. Configuramos la aplicación del OpenVPN para que establezca conexión con Nethserver de manera segura incorporando el certificado emitido por este mismo.



Fuente: Autoría Propia

3.5.3 Importancia de la VPN

La implementación de VPN se considera una solución esencial para mitigar riesgos de seguridad asociados al acceso remoto. Este servicio protege los datos corporativos contra ataques cibernéticos y garantiza la privacidad, especialmente cuando se utiliza desde redes públicas o no confiables. Según la documentación oficial de NethServer, su uso es indispensable en entornos empresariales para mantener la integridad de las comunicaciones internas [7][8].

4. CONCLUSIONES

La implementación de NethServer en una máquina virtual demostró ser una solución eficiente para construir una infraestructura de red robusta y segura. Se configuraron exitosamente servicios esenciales como DHCP, DNS, controlador de dominio, proxy web, firewall, servidor de archivos y servidor de impresión, optimizando la gestión de red y la seguridad.

La configuración del proxy web permitió filtrar el tráfico de internet, mientras que el firewall bloqueó el acceso a sitios no deseados, reforzando la seguridad de la red y promoviendo un entorno productivo.

El servidor de archivos y el servidor de impresión centralizaron la gestión de recursos compartidos, mejorando la eficiencia y el control de acceso.

La implementación de una VPN proporcionó una capa adicional de seguridad para el acceso remoto a la red, garantizando la privacidad y la integridad de las conexiones.

Las pruebas de validación confirmaron el correcto funcionamiento de cada servicio, demostrando que la infraestructura implementada cumple con los requisitos de seguridad y funcionalidad.

5. REFERENCIAS

- [1] M. C. Caballero [@DriveMeca], "Nethserver Tutorial | Instalación, actualización y primeros pasos," Youtube, [Online]. Available: https://www.youtube.com/watch?v=FNGmM-2fa_0. [Accessed: 03-Dec-2024].
- [2] "Carpetas compartidas — NethServer 7 Final," Nethserver.org, [Online]. Available: https://docs.nethserver.org/es/v7/shared_folder.html. [Accessed: 03-Dec-2024].
- [3] "DNS — NethServer 7 Final," Nethserver.org, [Online]. Available: <https://docs.nethserver.org/es/v7/dns.htm>. [Accessed: 03-Dec-2024].
- [4] "Firewall y gateway / Cortafuego y Puerta de enlace — NethServer 6.10 Final," Nethserver.org, [Online]. Available: <https://docs.nethserver.org/es/v6/firewall.html>. [Accessed: 03-Dec-2024].
- [5] "Nethserver-cups — NethServer 7 documentation," Nethserver.org, [Online]. Available: <https://docs.nethserver.org/projects/nethserver-devel/en/latest/nethserver-cups.html>. [Accessed: 03-Dec-2024].
- [6] "Proxy web — NethServer 7 Final," Nethserver.org, [Online]. Available: https://docs.nethserver.org/es/v7/web_proxy.html. [Accessed: 03-Dec-2024].
- [7] "VPN — NethServer 7 Final," Nethserver.org, [Online]. Available: <https://docs.nethserver.org/es/v7/vpn.html>. [Accessed: 03-Dec-2024].
- [8] "Getting started with Nethserver," Nethserver.org, [Online]. Available: <https://www.nethserver.org/getting-started-with-nethserver/>. [Accessed: 03-Dec-2024].